隐蔽通信网络传输信息加密处理方法

孙立仙[1]
SUN Lixian

摘 要 由于传统方法在隐蔽通信网络传输信息加密处理中应用效果不佳，加密处理后传输信息的隐蔽性指数较低，并且通信网络传输信息丢包率较高，无法达到预期的处理效果，提出隐蔽通信网络传输信息加密处理方法研究。首先利用自回归模型与移动平均模型建立通信网络异常检测模型；其次采用通信网络异常检测模型对通信网络波动偏离识别，检测传输信息异常；再次采用空域隐写算法对异常状态下通信网络传输信息进行隐蔽；最后利用蜜罐诱骗机制对通信网络入侵者引诱，将通信网络传输信息通过一维 Logitic 映射与二维 Tent 映射生成密文，对传输信息双层加密，以此实现隐蔽通信网络传输信息加密处理。经实验证明，在设计方法应用下通信网络传输信息隐蔽性能达到 40 dB 以上，通信网络传输信息丢包率在 1% 以下，有效保证了传输信息的隐蔽性和私密性，设计方法在隐蔽通信网络传输信息加密处理方面具有良好的应用前景。

关键词 隐蔽通信网络；传输信息；加密处理；蜜罐诱骗机制；一维 Logitic 映射；二维 Tent 映射

doi：10.3969/j.issn.1672-9528.2024.01.036

0 引言

网络技术和数字媒体技术持续发展，人们在享受到通信网络所带来便利的同时，也越来越依赖于它。然而，这也带来了一些新的风险和问题，在数字信息作品在创作完毕之后，必然会在通信网络上进行传播和交换，在此过程中，很可能会遭到不法分子的恶意复制、篡改、传播等行为侵害，进而使个人、企业的合法权益进行受到严重威胁。最近几年，通信网络市场的发展迅猛，在过去的五年中，通信网络市场规模已经翻了 12.5 倍。在通信网络环境中，由于使用了大规模分布式计算机来处理网络信息，而非本地计算机，通过对海量信息进行计算与传输，使信息资源能够更多地投入到所需要的通信应用上，实现数据交换。由于通信网络具有开放性特性，隐蔽性较差，信息传输过程中必然会存在一定的安全风险。而结合加密处理方法将有效解决通信网络信息传输中的安全问题，提高通信网络的隐蔽性，为信息的安全传输提供可能。但是由于通信网络传输信息量较大，且信息种类比较丰富，包括文字、图像、音频等，这在一定程度上提升了隐蔽通信网络传输信息加密处理难度。近几年通信网络传输信息安全问题受到研究领域的重视与关注，相关学者与专家开展了一系列研究。例如，马亚蕾等人提出基于区块链的隐蔽通信网络传输信息加密处理方法[1]，利用密码学算法生成一对公钥和私钥。首先当发送方想要向接收方发送信息时，使用接收方的公钥对信息进行加密。其次加密后的信息会被存储在区块链的交易中，发送到这个区块链网络。然后接收方会监控发送到自己的区块链交易，一旦发现有新的交易，就会提取出加密的信息。最后接收方使用自己的私钥对提取出的加密信息进行解密，得到原始信息。在这个过程中，即使攻击者能够监听、获取区块链交易数据，但由于他们无法获取到用户的私钥，因此无法解密出原始信息。另外，由于这种特殊的交易中的地址（发送地址和接收地址）以及数据与其他交易没有明显区别，攻击者也很难筛选出这些特殊的交易。此方法能的安全性得到提高，但是隐蔽性指数不高。

袁立等人提出基于哈希函数的隐蔽通信网络传输信息加密处理方法[2]，选择 SHA-256 哈希函数，将要传输的原始信息输入到哈希函数中，生成一个唯一的哈希值，这个哈希值可以被视为原始信息的“指纹”。在需要加密的文件中，将其格式文本中的排版或者其他特征进行调整，调整幅度根据需要加密文件的重要性来决定。这种调整必须是双方事先约定好的，以便接收方能够正确地解密。将生成的哈希值和调整后的文本一起传输，即使攻击者截获了传输的信息，他们也只能看到哈希值和看似无意义的调整后的文本，而不能得到原始信息。接收方收到信息后，通过同样的哈希函数对调整后的文本进行哈希，得到一个新的哈希值。将这个新的哈希值与传输过来的哈希值进行比较。如果两者相同，说明信

1. 朝阳师范高等专科学校 辽宁朝阳 122000

息没有被篡改，接收方就可以按照事先约定的方式对文本进行调整，以得到原始信息。此方法能够有效提升加密安全性，但是传输信息丢包率高。

针对上述方法存在传输信息丢包率高、隐蔽性指数不佳的问题，本文提出隐蔽通信网络传输信息加密处理方法。

1 建立通信网络异常检测模型

在隐蔽通信网络传输信息过程中，要对信息进行加密处理操作，利用时序分析方法来实现在通信网络信息传输中异常流量的识别与检测。本文通过自回归移动平均模型，由自回归模型（A 模型）与移动平均模型（MA 模型）两个部分进行组合而形成的，其中自回归模型用公式表示为：

$$C = e + \sum_{t=1}^{p} x_t + v \tag{1}$$

式中：C 表示自回归模型；e 表示常数项；p 表示阶数；t 表示通信网络传输信息时刻值；x_t 表示参数项；v 表示白噪声扰动项[3]。将通过网络异常流量识别指标按照时间顺序记录，使数据流形成一个数据列，根据数据列的依存关系描述出原始网络流量在时间上的连续性，利用时间序列建立移动平均模型，用公式表示为：

$$K = e + \sum_{t=1}^{p} \varphi_t + v \tag{2}$$

式中：K 表示移动平均模型；φ_t 表示参数项[4]。将以上建立的自回归模型与移动平均模型整合，建立自回归移动平均模型，用公式表示为：

$$G = C + XK \tag{3}$$

式中：G 表示自回归移动平均模型；X 表示随机变量。为了能够更好地检测到通信网络中传输信息异常流量，通过自回归移动平均模型来进行异常点的探测，并对其进行预报[5]。在对网络进行检测前，需要获取通信网络数据的传播特征。根据通信网络的传递时序图来判断其是否正常[6]，若通信网络中存在异常的时间序列，则对其进行差分处理，进而再利用自回归移动平均模型，在此基础上对通信网络异常流量进行识别，其检测过程如下。

考虑到自回归移动平均模型在对通信网络异常流量检测过程中，会受到外界因素以及模型自身变动规律等因素影响，故利用上文建立的基础模型，即公式（3）对通信网络传输数据流进行回归分析，用公式表示为：

$$T(G) = \alpha_0 + \alpha_1 x_1 + \cdots + \alpha_k x_k \tag{4}$$

式中：$T(G)$ 表示模型检测对象的观测值；$\alpha_k x_k$ 表示第 k 个影响因素和其对应的影响系数[7]。当不同时期因存在白噪声造成自回归移动平均模型扰动误差存在依存关系时，得到自回归移动平均模型扰动误差，根据扰动误差对上文建立的自回归移动平均模型优化，消除扰动误差，建立模型用公式表示为：

$$G^* = 2e + \sum_{t=1}^{p} x_t^{T(G)} + \sum_{t=1}^{p} \varphi_t^{T(G)} \tag{5}$$

式中：G^* 表示优化后的自回归移动平均模型，该模型为通信网络异常检测模型，用于后续网络波动偏离识别与分析。

2 通信网络波动偏离识别

当网络通信过程出现异常波动，将导致通信网络异常检测模型传播特性发生变化，分析通信网络异常检测模型传输时序偏离度，完成通信网络波动异常识别[8]。在通信网络网中，利用残差表示出通信网络信息传输偏差，将通信网络波动偏离度定义为信息传输残差，选择一组正常状态下通信网络传输信息，将其与当前通信网络传输信息对比，分析得到传输偏离度，确定通信网络信息传输的残差序列，确定当前时刻通信网络信息传输残差值，并对其进行周期性更新[9]。

因为在本次研究中，网络传播残差序列所表现出来的特性并不与平稳时间序列的特性相匹配，对序列进行平稳化处理，也就是对原序列进行一次或几次差分，将其转化为平稳序列之后，采用通信网络异常检测模型对时间序列的波动性进行仿真分析，得到与其波动性一致的时间序列。

随机选取一组通信网络传输信息样本，将其代入到通信网络异常检测模型中，对模型进行拟合，确定模型参数。假设通信网络传输信息残差序列为 $N=n_1, n_2, \cdots, n_m$，利用拟合后的通信网络异常检测模型对传输时间序列异常偏离度计算，用公式表示为：

$$\gamma_t = G^* \exp\frac{\left|c_t - \overline{c_{t-1}}\right|}{h} \tag{6}$$

式中：γ_t 表示在当前时刻通信网络传输信息时间序列异常偏离度；c_t 表示通信网络传输信息时间残差；$\overline{c_{t-1}}$ 表示在上一时刻的通信网络传输信息时间残差均值；h 表示通信网络传输信息时间标准差。将计算到的异常偏离度与阈值比较，如果小于阈值，则说明当前时刻通信网络传输信息正常；如果大于阈值，则说明当前时刻通信网络传输信息波动异常，以此识别检测到通信网络异常波动状态。

3 传输信息空域隐写

当识别检测到通信网络传输信息波动异常，对通信网络传输信息进行隐蔽处理，提升通信网络的隐蔽性，采用空域隐写算法对通信网络传输信息进行隐蔽，空域隐写算法原理是将传输信息转换为二进制，将信息嵌入到图像中，将图像

作为信息隐蔽载体，用公式表示为：

$$d=\varepsilon+z^{\gamma_t} \tag{7}$$

式中：d 表示空域隐写处理后的通信网络传输信息；ε 表示载密图像像素值；z^{γ_t} 表示通信网络传输信息比特 [10]。利用上述公式将通信网络传输信息嵌入到数字图像中，实现对传输信息的隐蔽。

4 传输信息双层加密处理

建立通信网络传输信息双层加密处理机制，该机制由蜜罐诱骗和信息加密两部分组成，为了保证传输信息的私密性，在信息加密的同时利用蜜罐诱骗机制对通信网络入侵黑客进行引诱，蜜罐引诱包括信息外表伪装、简单进入、传输过程伪装以及伪信息诱骗四部分，根据原传输信息内容生成用于蜜罐诱骗的伪信息，用公式表示为：

$$\psi(x)=d\cdot\beta+F\kappa^{d} \tag{8}$$

式中：$\psi(x)$ 表示用于蜜罐诱骗的伪信息；β 表示传输信息的序列数；F 表示伪信息生成函数；κ^{d} 表示伪信息字符串 [11]。首先利用式（8）生成传输信息的伪信息，用生成的伪信息对通信网络入侵者进行诱骗，对通信网络端口进行蜜罐伪装。其次通过模拟通信网络入侵特征，在通信网络布设一个伪装端口，用于网络入侵者进入到通信网络后对端口扫描操作 [12]。再次，为了降低入侵者从伪装端口入侵门槛，将伪装断口的密码设置为简单的数字密码 [13]。然后在蜜罐中为入侵者提供伪装的网络传输服务，使蜜罐看起来是一个正常的外部通信节点 [14]。最后将生成的伪信息分配到通信节点上，入侵者进入到蜜罐后可以获取到伪信息，以此成功诱骗入侵者对伪信息的截获，使其停留在蜜罐中。

为了进一步保证传输信息安全，防止入侵者破解上文建立的蜜罐诱骗机制，对传输信息进行双层加密，其过程如下。

步骤 1：明文信息空间映射。通过对传输信息传入到分布式编辑器中，对传输信息明文进行编码处理，利用概率密度函数将传输信息明文映射到种子空间中，用公式表示为：

$$\omega\leftarrow encode(H) \tag{9}$$

式中：ω 表示映射到种子空间中传输信息明文；$encode$ 表示空间搜索信息输出值；H 表示分布式编辑器输出值。

步骤 2：基于一维 Logitic 映射的明文首层加密 [15]。利用一维 Logitic 映射算法将种子空间中的明文信息映射到一维空间中，结合上文生成的用于蜜罐诱骗的伪信息生成首层加密密文，用公式表示为：

$$I=\psi(x)(\omega,\phi) \tag{10}$$

式中：I 表示隐蔽通信网络传输信息首层加密密文；ϕ 表示归一化处理后的加密口令 [16]。通过以上处理实现对隐蔽通信网络传输信息首层加密处理。

步骤 3：基于二维 Tent 映射的明文二层加密处理 [17]。利用二维 Tent 映射算法将首层加密后的密文进行二层加密处理，生成二层加密密文，用公式表示为：

$$W=I(\chi,\xi) \tag{11}$$

式中：W 表示隐蔽通信网络传输信息二层加密密文；χ 表示给定的口令；ξ 表示给定的隐蔽通信网络传输信息字符串 [18]。利用上述公式，将通信网络传输信息映射到二维空间中，完成对传输信息二层加密。当通信网络入侵者破解了蜜罐诱骗机制后，采用一维 Logitic 映射与二维 Tent 映射，将通信网络传输信息进行双层加密处理，入侵者如果需要得到明文，则要对其进行两层解密计算，但即使完成双层解密计算，也是获得经过隐蔽处理后的通信网络传输信息的伪信息。正常用户按照以上加密过程进行逆计算，即可实现对传输信息的解密处理，获取到传输信息明文，进而实现了隐蔽通信网络传输信息加密处理，通信网络中加密信息的传输流程如图 1 所示。

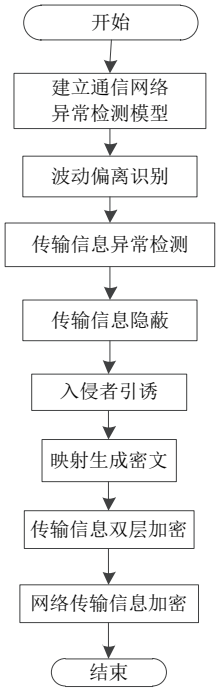


图 1 加密信息传输流程图

5 实验与分析

5.1 实验环境与设置

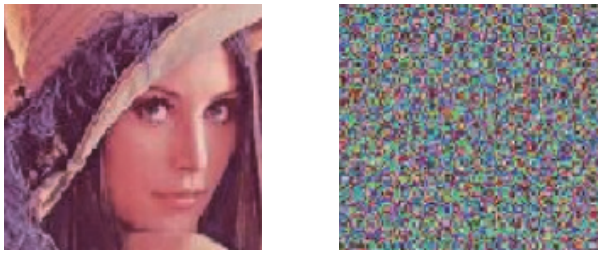
针对以上提出方法，选择 KHFATWART 与 RQWTWJAI 数据包对所提方法隐蔽通信网络传输信息加密处理性能检验，KHFATWART 数据包主要为图像数据，数据总量为 10 000 Byte，RQWTWJAI 数据包主要为文字数据，数据总量为 5000 Byte。根据需求布设实验环境，采用 Windows

server 2010 作为隐蔽通信网络传输信息加密处理的操作系统，采用 intel coer 5-6410 128 GB i8 处理器，启动开发工具 SDSoc2020，在 KHFATWART 与 RQWTWJAI 数据集中随机抽取数据作为数据样本，用于通信网络传输。通信网络通信用户数量为 100 个，网络信息传输次数设置为 1000 次，通信网络访问频率为 1.52 GHz。为了使实验环境模拟更加真实，在通信网络中引入 siyfasf 与 IYUFAH 两种波动，波动频率设置为 152.16 kHz，并在通信网络信息传输中设置 500 个病毒攻击样本数，通信网络信噪比设置为 1.62 dB，以该实验环境为基础，开展实验研究。随机选择一组本文信息，其加密过程如表 1 所示。

表 1 明文块加密过程

Ji	Ri	Ei	Wi
261552614	4514415157	84555E4541	481451W125
152552553	1445242274	1522559944	1523459185
625414J15	4582252552	5966856652	1536456854
451296258	1525842551	15335i2552	1233525515
263255352	45522R4842	1522355214	2568455152
2952i5922	155i251225	1521455155	1523651155
861851565	4865755552	1533548525	0354168424
292654564	5929988555	7894895666	4822361554

如表 1 所示，传输信息文明块加密后由 8 组数据序列组成，密文复杂程度较高。对于图像加密处理，随机选择一张图像信息样本，图像信息加密处理前后如图 2 所示。



加密前　　加密后

图 2 图像信息加密结果

对加密后的信息传输，实验共传输 5 个图像流量包和 5 个文字流量包，统计加密后隐蔽通信网络传输信息丢失量和无效数据量，如表 2 所示。

表 2 隐蔽通信网络信息加密后传输结果

网络流量包	大小 /Byte	丢失数据量	无效数据量
图像 1	2000	12.06	0.14
图像 2	2000	12.52	0.24
图像 3	2000	11.43	0.16
图像 4	2000	10.62	0.24
图像 5	2000	10.42	0.13
文字 1	1000	15.15	0.24
文字 2	1000	12.36	0.36
文字 3	1000	14.15	0.14
文字 4	1000	12.45	0.22
文字 5	1000	16.25	0.24

基于以上实验结果，开展实验结果讨论分析。

5.2 实验结果与讨论

5.2.1 实验方法

基于区块链的隐蔽通信网络传输信息加密处理方法（OURA）与基于哈希函数的隐蔽通信网络传输信息加密处理方法（HFQA）为目前现实中比较常用的处理方法，OURA 是利用区块链技术将传输信息在区块中进行加密处理；HFQA 是利用哈希函数计算传输信息的哈希值生成密文，实现对传输信息加密处理，选择以上两种方法作为比较，完成对比实验。

5.2.2 实验指标选择

（1）信息传输安全性

验证本文所提方法的传输安全性，首先在通信网络信息传输过程中注入一定网络攻击，然后根据攻击后的传输路径自愈能力来判断信息传输的安全性，通信网络节点中注入攻击的位置如图 3 所示。

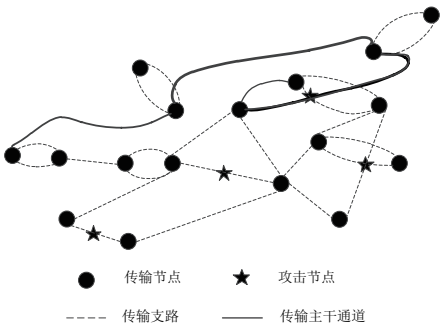


图 3 网络攻击下的通信网络示意图

当受到攻击的传输通道能够实现自愈传输后，表明通信网络传输安全性高，实现了传输信息加密处理目的。

（2）隐蔽性指数（R）

隐蔽通信网络传输信息加密处理效果，可以通过信息的隐蔽性指数（R）与丢包率表现出来，R 值越大，说明加密处理后的信息隐蔽性越好，安全性越高，其计算公式为：

$$R=10\times\lg\left(\frac{M^2}{D}\right) \tag{12}$$

式中：R 表示隐蔽通信网络传输信息的隐蔽性指数；M 表示隐蔽通信网络传输信息的峰值信噪比；D 表示载密信息与载体信息的均方差。

（3）丢包率

利用 KHFATWART 数据包对信息加密处理方法的隐蔽性能验证。丢包率表示网络传输丢失信息比例，其计算公式为：

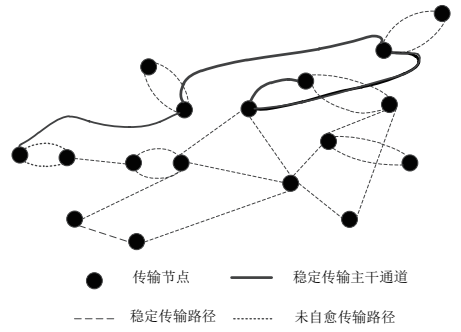
$$J=\frac{E+S}{W}\times 100\% \tag{13}$$

式中：J 表示隐蔽通信网络传输信息丢包率；E 表示丢失信息数量；S 表示无效信息数量；W 隐蔽通信网络传输流量大小。

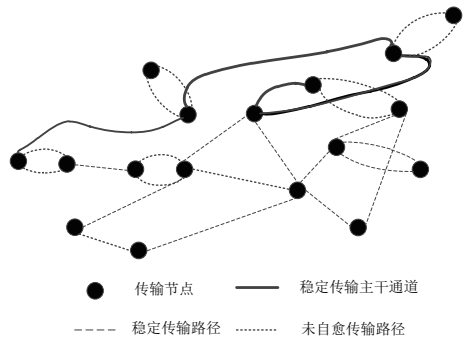
5.2.3 结果分析

（1）信息传输安全性

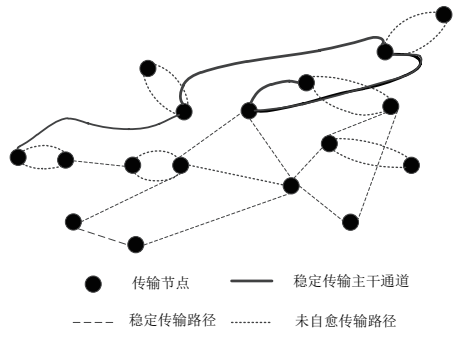
在设计的通信网络攻击基础上，应用上述文中所提的三种通信网络传输方法后，测试通信网络自愈能力的结果模拟图如 4 所示。



（a）本文方法



（b）OURA 方法



（c）HFQA 方法

图 4 通信网络传输路径自愈对比图

由图 4 可知，在基 OURA 传输方法与 HFQA 传输方法中，存在多条未自愈的传输路径，无法恢复为原始传输状态；而本文所提方法在攻击后，传输路径可以较好的自愈，恢复到原始传输状态，保障了通信网络信息传输的安全性。通过上述实验结果，可以充分验证本文所提基于数据加密技术的通信网络信息传输方法的可靠性。

（2）PSNR

利用 RQWTWJAI 数据包对加密处理方法的 PSNR 性能验证，得到实验结果如图 5 所示。

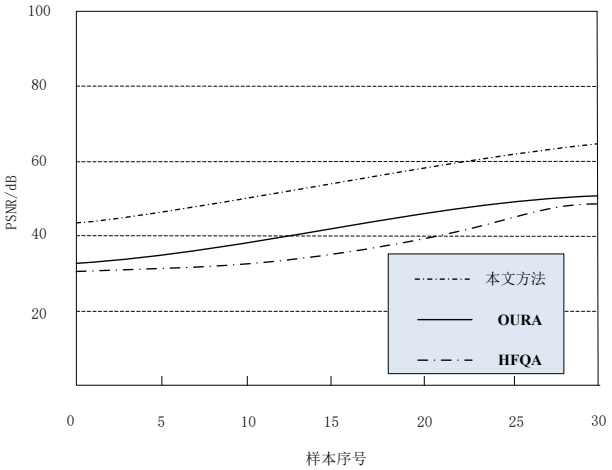


图 5 隐蔽通信网络传输信息 PSNR

从图 5 可以看出，30 个传输信息样本，三种方法表现的 PSNR 性能存在差异，设计方法 PSNR 平均值为 45.05 dB，OURA 的 PSNR 平均值为 39.56 dB，HFQA 的 PSNR 平均值为 34.12 dB，从数值上看 HFQA 的传输信息隐蔽性最低，设计方法的传输信息隐蔽性最高，证明本文方法在加密处理后信息隐蔽性性能最优。

（3）丢包率

利用 RQWTWJAI 数据包对加密处理方法的丢包率性能验证，得到实验结果如表 3 所示。

表 3 隐蔽通信网络传输信息丢包率 /%

信息量 /Byte	本文方法	OURA	HFQA
1000	0.35	5.15	6.12
2000	0.36	5.24	6.22
3000	0.33	5.26	6.21
4000	0.34	5.31	6.25
5000	0.36	5.32	6.27
6000	0.35	5.33	6.35
7000	0.35	5.52	6.36
8000	0.36	5.14	6.52
9000	0.37	5.16	6.25
10 000	0.39	5.24	6.34

基于表 3 中数据分析，本文方法隐蔽通信网络传输信息丢包率最高值为 0.39%，OURA 隐蔽通信网络传输信息丢包率最高值为 5.52%，HFQA 隐蔽通信网络传输信息丢包率最高值为 6.34%，从数值上看 HFQA 的丢包率最高，本文方法最低。出现以上差异，是因为设计方法采用了隐写算法将传输信息嵌入到图像中，提高了传输信息的隐蔽性，并采用回归平移平均模型对通信网络异常进行检测。根据网络实时情况对传输信息通过一维 Logitic 映射与二维 Tent 映射，实现传输信息的双层加密，以此保证传输信息的安全性和私密性。通过以上对比和分析，证明了设计方法加密处理效果良好，能够有效保证通信网络的隐蔽性以及传输信息的安全性，具有良好的适用性。

6 结语

现如今人们对通信网络的隐蔽性要求以及传输信息的私密性要求越来越高，由于传输信息量庞大，信息传输过程中很容易受到攻击，针对隐蔽通信网络传输信息安全加密问题，此次参考相关文献资料，融合多种信息化技术，针对现行方法存在的不足与缺陷，提出隐蔽通信网络传输信息加密处理方法，有效提高了通信网络的隐蔽性以及传输信息的安全性和私密性，提高了隐蔽通信网络传输信息加密处理质量，为实际信息加密处理提供了有力的理论支撑，同时也为隐蔽通信网络传输信息加密处理方法研究提供了参考依据。由于此次研究精力和时间有限，研究方法目前尚处于初步探索阶段，尚未在实际中得到大量的实践与应用，在某些方面或许存在不足，今后会加深对该方面研究的同时，还会在隐蔽通信网络传输信息安全检测等方面展开研究，促进通信网络技术又好又快发展。

参考文献：

[1] 马亚蕾 , 张怡 . 基于区块链的通信网络节点位置隐私加密控制模型设计 [J]. 计算机测量与控制 , 2023, 31(4):246-251.

[2] 袁立 , 谢俐 , 龙颖 , 等 . 基于哈希和 DNA 编码的彩色图像混沌加密算法 [J]. 重庆大学学报 , 2021,44(7):55-63.

[3] 田如意 , 顾风军 , 彭坤 , 等 . 基于一维 Logistic 映射和二维 Tent 映射双混沌思路的网络信息加密 [J]. 计算机测量与控制 , 2023, 31(6):280-286.

[4] 刘洪鑫 , 徐非非 , 黄剑 . 基于蜜罐机制的电力调度信息加密传输方法研究 [J]. 电子设计工程 , 2023, 31(7): 32-35+41.

[5] 邢宇航 , 王利涛 , 李敏 , 等 . 一种基于 RS485 的信息加密传输装置设计与实现 [J]. 信息记录材料 ,2023,24(3):139-141+146.

[6] 林钰达 , 金梁 , 黄开枝 , 等 . 基于多径信道能量随机动态打散的隐蔽无线通信方案 [J]. 电子与信息学报 , 2023, 45(2): 505-515.

[7] 周力 . 基于 AES 算法的网络通信信息加密传输技术研究 [J]. 长江信息通信 ,2023,36(1):70-72.

[8] 杨娜 . 基于分组密码算法的网络传输数据信息加密方法研究 [J]. 信息与电脑（理论版）,2022,34(17):210-212.

[9] 熊礼治 , 朱蓉 , 付章杰 . 基于交易构造和转发机制的区块链网络隐蔽通信方法 [J]. 通信学报 , 2022, 43(8):176-187.

[10] 周小波 , 于辉 , 彭旭 , 等 . 智能反射面辅助及人工噪声增强的无线隐蔽通信 [J]. 电子与信息学报 , 2022, 44(7): 2392-2399.

[11] 佘维 , 霍丽娟 , 刘炜 , 等 . 一种可隐藏敏感文档和发送者身份的区块链隐蔽通信模型 [J]. 电子学报 , 2022, 50(4): 1002-1013.

[12] 王剑锋 , 林永峰 . 基于神经网络的电力调度信息加密传输方法研究 [J]. 微型电脑应用 , 2022,38(1):134-138.

[13] 蒋岑 , 吴迪 . 隐蔽无线通信网络传输信息云存储密文检索 [J]. 计算机仿真 , 2021,38(6):125-128+137.

[14] 周泽岩 . 基于直觉模糊集的网络信息加密传输方法 [J]. 信息与电脑 (理论版), 2021,33(6):42-44.

[15] 赵悦品 , 孙洁丽 . 船用物联网中的信息安全传输系统 [J]. 舰船科学技术 , 2020,42(20):202-204.

[16] 倪磊 , 达新宇 , 胡航 , 等 . 基于 MP-WFRFT 的多维联合调制卫星隐蔽通信研究 [J]. 电子与信息学报 , 2023, 45(4): 1183-1191.

[17] 冯娜 . 基于物联网中传输层图像信息加密及压缩的算法探讨 [J]. 黑龙江工业学院学报 (综合版), 2020, 20(4): 85-88.

[18] 张忠山 . 舰船电子系统信息传输单向防御加密技术 [J]. 舰船科学技术 , 2020,42(6):181-183.

【作者简介】

孙立仙（1972—），男，辽宁朝阳人，本科，高级实验师，研究方向：计算机、网络。

（收稿日期：2023-10-13）